| | |
|---|---|
| *On behalf of* | *: First Defendant* |
| *Witness* | *: Oliver Robbins* |
| *No. of statement:* | *: 1* |
| *Dated* | *: 27 August 2013* |

CO/11732/2013

IN THE HIGH COURT OF JUSTICE

QUEEN'S BENCH DIVISION

ADMINISTRATIVE COURT

R

on the application of

DAVID MICHAEL DOS SANTOS MIRANDA

Claimant

and

(1) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(2) COMMISSIONER OF POLICE FOR THE METROPOLIS

Defendants

---

First Witness Statement of Oliver Robbins

---

I, Oliver Robbins, of 70 Whitehall, London SW1A 2AS **WILL SAY** as follows:

1. I am the Deputy National Security Adviser for Intelligence, Security and Resilience in the Cabinet Office. I report directly to the Prime Minister, the National Security Council and the National Security Adviser, Sir Kim Darroch.

2. I have been a member of the civil service for the last 17 years and am a Senior Civil Servant. I have served in a number of roles across government, including serving as the Prime Minister's Principal Private Secretary.

3. In my current role I am responsible for policy, resourcing and capability matters relating to the United Kingdom's security and intelligence agencies. I oversee the annual setting of the security and intelligence agencies' requirements and priorities and I represent the United Kingdom in international intelligence and security fora. I advise the National Security Council on counter-terrorism and counter-espionage issues. I am also responsible for managing the United Kingdom's crisis management machinery, for producing the Government's security policies (including those which govern protection of the assets of the security and intelligence agencies) and I manage the UK's National Cyber Security Programme.

4. I am authorised to make this witness statement on behalf of the first defendant in opposition to the claimant's application for interim relief in these proceedings. I make this statement from my own knowledge and where matters are not within my own knowledge from information and documentation made available to me and from consultations with other parts of Government. The facts set out in this statement are true to the best of my knowledge and belief.

5. This witness statement seeks to outline why the defendants need to make use of the material that was detained pursuant to paragraph 11 of Schedule 7 to the Terrorism Act 2000, pending final determination of these proceedings and the risk to national security if the interim relief sought by the claimant is granted. Specifically, this statement explains:
    - the background to the material seized;
    - HMG's best assessment in an open statement of the harm we fear would be caused by disclosure of the material seized;
    - as an example of this damage, the concern we have to protect intelligence officer identities;
    - why HMG needs continuing access to the material to mitigate current and future risks to national security;
    - how this access also supports the continuing criminal investigation;
    - why it would further risk national security to return the material; and
    - HMG's approach to the material held by The Guardian newspaper, which the claimant alleges is inconsistent.

6. I would like to make clear at the outset that no information that has so far been analysed by Her Majesty's Government ("HMG") has identified a journalist source or has contained any items prepared by a journalist with a view to publication. The information that has been accessed consists entirely of misappropriated classified material in the form of approximately 58,000 highly classified UK intelligence documents. I can confirm that the disclosure of this information would cause harm to UK national security.

**Background**

7. The claimant is the partner of Glenn Greenwald, who writes for (amongst other publications) The Guardian newspaper. There are two other individuals who are relevant to the background of the present action, Laura Poitras and Edward Snowden.

8. Mr Snowden was a former employee of the US Central Intelligence Agency ("CIA") and a contractor to the National Security Agency ("NSA"). It has been reported that Mr Snowden was able to obtain a vast amount of classified material during his employment. Ms Poitras is a documentary film maker, who, along with Mr Greenwald, is believed to have access to this intelligence information.

9. There has been a great deal of open source reporting concerning the classified material that was obtained by Mr Snowden and the roles of the claimant, Mr Greenwald and Ms Poitras. In describing the background to the circumstances of this claim I will therefore refer to this open source material.

10. In a newspaper article published by The Guardian on 19 August 2013 ("Glenn Greenwald: detaining my partner was a failed attempt at intimidation"), Mr Greenwald stated that the claimant had spent the week before his detention at Heathrow Airport in Berlin, where he stayed with Ms Poitras, whom he described as having worked with him extensively on the stories relating to surveillance by the NSA.

11. In an article published on the same day by the Columbia Journalism Review ("Guardian bombshells in an escalating battle against journalism") Ryan Chittum wrote that the claimant "was serving as a human passenger pigeon, shuttling encrypted files on USB drives between filmmaker Laura Poitras and Greenwald". The statement that the claimant was acting as a courier between Mr Greenwald and Ms Poitras was repeated by Joel Simon, Executive Director of the Committee to Protect Journalists, in his letter of 20 August to the Prime Minister. In an article published in The New York Times on 13 August ("How Laura Poitras helped Snowden spill his secrets") Peter Maass stated that Mr Snowden gave Ms Poitras and

Mr Greenwald "thousands of classified documents", and that Ms Poitras and Mr Greenwald "have not shared the full set of documents with anyone".

12. Media reporting has suggested that the only complete copies of the classified material shared with them by Mr Snowden are still held by Ms Poitras, in Germany, and Mr Greenwald, in Brazil. HMG were aware that The Guardian possessed a subset of the material, although we do not know how much.

13. I am advised that the data recovered from the claimant is almost certain to contain some of the material passed by Mr Snowden to Ms Poitras and Mr Greenwald. Much of the material is encrypted. However, among the unencrypted documents recovered from the claimant was a piece of paper containing basic instructions for accessing some data, together with a piece of paper that included the password for decrypting one of the encrypted files on the external hard drive recovered from the claimant. I have been briefed that the authorities have therefore been able to examine the data contained in this file. They have been able to determine that the external hard drive contains approximately 58,000 highly classified UK intelligence documents. Work continues to access the content of the other files on the hard drive and the USB sticks.

14. The New York Times article by Peter Maass cited above states that Mr Snowden had access to "not just a few secrets but thousands of them, because of [his] ability to scrape classified networks". "Scraping" in this context refers to the automated bulk downloading of material from a website or a network. On the basis of GCHQ assessments, the totality of UK intelligence documents that would potentially have been accessible to Mr Snowden while he was working at the NSA is consistent with the volume of documents which we know to be on the external hard drive. HMG believes, therefore, that far from undertaking targeted and careful appropriation of classified material, Mr Snowden indiscriminately appropriated material in bulk and that this information, or at least some of it, is the same material that the claimant was couriering for Mr Greenwald.

**Risk to National Security – general**

15. It is not possible in an open statement to get into detail about the real and serious damage already caused by the disclosures made based on Mr Snowden's misappropriations, nor about what damage could ensue if the material seized from the claimant were disclosed. However, given the volume of open source reporting, and recent public statements from senior officials

in both HMG and the US Government, I can say with confidence in this statement that the material seized is highly likely to describe techniques which have been crucial in life-saving counter-terrorist operations, and other intelligence activities vital to UK national security. The compromise of these methods would do serious damage to UK national security, and ultimately risk lives.

16. For security and intelligence agencies engaged in covert activities to ensure the national security of the United Kingdom, the protection of staff identities is critical to their operational effectiveness and overall ability to discharge their statutory duties. Anything that reveals or indicates the identities of members of UK security and intelligence agencies would be of value to elements hostile to the national interest of the United Kingdom, including foreign intelligence agencies and terrorists who actively seek such information. The interim relief sought by the claimant would prevent urgent work to understand the magnitude of this risk and, in particular, the ability to take steps to mitigate that risk. Greater detail on this specific example is provided in paragraph 19 onwards below.

17. In general terms, it can be said that a large proportion of the material is classified either at SECRET or TOP SECRET. According to the Security Policy Framework, the compromise of SECRET information would be likely to have one or more of the following consequences: to raise international tension; seriously to damage relations with friendly governments; to threaten life directly or seriously prejudice public order, or individual security or liberty; to cause serious damage to the operational effectiveness of highly valuable security or intelligence operations; and to cause substantial material damage to national finances or economic and commercial interests. The compromise of TOP SECRET information would be likely to have one or more of the following consequences: to threaten the internal stability of the UK or friendly countries; to lead directly to widespread loss of life; to cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of security or intelligence operations; to cause exceptionally grave damage to relations with friendly governments; and to cause severe long-term damage to the UK economy.

18. The effect of disclosure is outlined in public guidance issued by the Defence, Press and Broadcasting Advisory Committee (DPBAC) which oversees a voluntary code which operates between HMG and the media for the purpose of preventing inadvertent disclosure of information that would compromise UK military and intelligence operations and methods, or put at risk those involved or endanger lives; and which guides the media to seek advice for material falling within this category. Notice DA-05 of this code is as follows:

"Identified staff from the intelligence and security services, others engaged on sensitive counter-terrorist operations, including the Special Forces, and those who are likely targets for attack are at real risk from terrorists. Security and intelligence operations contacts and techniques are easily compromised, and therefore need to be pursued in conditions of secrecy. Publicity about an operation which is in train finishes it. Publicity given even to an operation which has been completed, whether successfully or not, may well deny the opportunity for further exploitation of a capability, which may be unique against other hostile and illegal activity. The disclosure of identities can prejudice past, present and future operations. Even inaccurate speculation about the source of information on a given issue can put intelligence operations (and, in the worst cases, lives at risk and/or lead to the loss of information which is important in the interests of national security. Material which has been the subject of an official announcement is not covered by this notice."

**Risk to National Security - an example**

19. A particular concern for HMG is the possibility that the identity of a UK intelligence officer might be revealed. It is known that contained in the seized material are personal information that would allow staff to be identified, including those deployed overseas. It would cause real harm to the work of the UK's security and intelligence agencies if an intelligence officer were to have his or her identity disclosed on anything other than an authorised and limited basis.

20. It is necessary for members of the UK intelligence agencies to continue to remain anonymous as public identification of an officer could restrict the effectiveness of that individual in his or her job, compromise others (including current and previous operations) or result in danger to the persons concerned or their close associates. In a variety of circumstances, this danger includes a risk to life, both to intelligence officers and their families and recruitment attempts or threats to their safety by hostile intelligence services or terrorist groups.

21. In respect of the threat from hostile intelligence services, HMG has had to assume that copies of the information held by Mr Snowden may be held by one or more other States having regard to Mr Snowden's travel since leaving the United States. Given the variety of threats, and the risk of abuse of the information relating to staff identities contained in the material seized, I am advised that the information that has already been obtained has had a direct impact on decisions taken in regard to staff deployments and is therefore impacting operational effectiveness. Ongoing risk assessment work is required to limit or pre-empt damage to national security. A fuller understanding of the totality of the data recovered from the claimant will not of itself reduce this risk, but will enable HMG to conduct more accurate risk assessments and to take steps accordingly.

**Continued access to the information**

22. Continued access to, and analysis of, the detained material is required to understand how it has been used and/or accessed to inform urgent action to protect UK national security. In conducting this work it may be necessary to make additional copies of the data or to otherwise afford greater access to it to allow more individuals to work on it or more technology to be applied to it. It is important to emphasise to the court that I have been briefed that this is not a simple process and, even given the very high priority that is being placed on the work (which is, of course, diverting resources within the security and intelligence agencies), this will take a considerable amount of time and will consume a large amount of resources.

23. While our examination of the file that we have decrypted has allowed us to determine that it contains what we assess might be a complete set of the UK intelligence documents held on one particular network, we have not identified within this file the documentary basis for articles written by Mr Greenwald based on US intelligence documents (e.g. "NSA Prism program taps in to user data of Apple, Google and others", The Guardian, 7 June). We believe that it is likely that some or all of this US material is contained in the data held on the USB sticks recovered from the claimant. We cannot rule out the possibility that additional UK material, for example highly classified intelligence reporting held on other networks to which HMG does not have direct access, may be included within it. We are seeking to decrypt this data.

24. It is not presently known how many copies of the material appropriated by Mr Snowden in fact exist or exactly who holds them, but – as mentioned above - it is assessed that copies may be held by one or more other States having regard to Mr Snowden's travel since leaving the United States. Continued access to the material is therefore essential to try to establish what threat to national security exists by virtue of the possession of this material by another State. We urgently need to identify and to understand the entirety of the material recovered from the claimant in order to assess the risks to sensitive intelligence sources and methods, and the threat to intelligence agency staff should their identities or details of their operational tradecraft be obtained by hostile actors.

**Return of the information**

25. I understand that the claimant is not seeking the return of the detained property as part of the interim relief. However, in order to assist the court, I will also outline why the return of this information would damage national security.

26. Neither Mr Snowden nor Mr Greenwald has sufficient understanding of the work of the UK security and intelligence agencies to be able to form a reliable judgement on what might or might not, if published, damage the national security of the United Kingdom, whether the publication is based on UK intelligence material or US intelligence material. Indeed it is impossible for a journalist alone to form a proper judgment about what disclosure of protectively marked intelligence does or does not damage national security (hence the longstanding Defence Advisory system described in paragraph 18, above). The fragmentary nature of intelligence means that even a seemingly innocuous piece of information can provide important clues to individuals involved in extremism or terrorism.

27. There is therefore a real risk that publication or disclosure of the information could cause unintended damage to that national security. It is worth reiterating the point that real damage has in fact already been done to UK national security by the media revelations (both in the UK and internationally).

28. Even if the claimant were to undertake not to publish or disclose the information that has been detained, the claimant and his associates have demonstrated very poor judgement in their security arrangements with respect to the material rendering the appropriation of the material, or at least access to it by other, non-State actors, a real possibility.

29. From what has been published in the media, Mr Greenwald does not apply good information security practice. An article published in the New York Times on 6 June 2013 ("Blogger, with a focus on surveillance, is at center of a debate") noted that "Mr Greenwald has said he has had to get up to speed in the security precautions that are expected from a reporter covering national security matters, including installing encrypted instant chat and e-mail programmes." The article quotes Mr Greenwald as saying "I am borderline illiterate on these matters, but I had somebody who is really well-regarded actually come and physically do my whole computer". The New York Times article of 13 August referred to above describes Mr Greenwald's handling of material supplied to him by Mr Snowden while travelling to Hong Kong: "On the plane, Greenwald began going through its contents, eventually coming across a secret court order requiring Verizon to give its customer phone records to the N.S.A...

Poitras, sitting 20 rows behind Greenwald, occasionally went forward to talk about what he was reading.... At times, they talked so animatedly that they disturbed passengers who were trying to sleep".

30. The fact that, as described earlier in paragraph 13, when arriving at Heathrow airport on 18 August the claimant was carrying on his person a handwritten a piece of paper containing the password for one of the encrypted files recovered from him is a sign of very poor information security practice. Such practices should be considered against the background of the practices of the security and intelligence agencies from which the material originates, where great lengths are gone to with a view to protecting such information. This is achieved through a combination of personnel security, physical security and information security.

31. The retention by the defendants of the material seized from the claimant would effectively remove the risk of its appropriation by others and would put it beyond the reach of hostile intelligence services and non-state actors. It should be noted that the principal reason behind the destruction of the material held by The Guardian was to address the risk of that material being obtained by others, especially hostile intelligence services.

**Criminal investigation**

32. At the Divisional Court hearing on 23 August 2013, the Metropolitan Police Service announced that it had started a criminal investigation. As will be set out in the second defendant's statement that is due to be served today, the effect of the order sought by the claimant would be to prevent the police from performing their core function: the prevention and detection of crime. The police do not have the same level of experience, expertise and technical capability as third parties, in particular GCHQ, which are necessary to access the data held on the electronic media seized by the second defendant. It is, therefore, essential that both the police and third parties are able to work on the electronic media and the data it contains for the purposes of the criminal investigation and to use as evidence in criminal proceedings.

33. The claimant has sought disclosure of the identity of any third party to whom access has been given to any of the material and of what material has been disclosed to such third parties. As is clear from this witness statement, the Metropolitan Police Service has given GCHQ access to the data to assist the police in the performance of its statutory duties. The Metropolitan Police Service has also requested support from the UK's National Technical Assistance Centre ("NTAC"). NTAC (which is formally part of GCHQ) provides law enforcement

agencies with a central facility for the complex processing of encrypted material, including through the application of enhanced capabilities and techniques, to derive evidence from seized electronic data.

34. The police have also provided the material to the UK intelligence agencies under section 19 of the Counter-Terrorism Act 2008 which provides that a person may disclose information to the any of the intelligence services (meaning the Security Service, the Secret Intelligence Service and GCHQ) for the purposes of the exercise by that service of its specified functions. The UK intelligence agencies may, in turn, disclose the information to a third party, including selected foreign parties, in the exercise of their statutory functions. It may well be necessary to disclose or provide access to the material seized by the police to foreign third parties to support the UK intelligence agencies' ability to access and to interpret the electronic media. This will, in turn, facilitate the second defendant's criminal investigation and support and inform action to protect the UK's national security. It is HMG's longstanding practice not to comment on the detail of intelligence exchanges with foreign partners, on the grounds that doing so even in a limited and apparently harmless way would risk undermining the immediacy and candour of such exchanges by raising fears among our partners as to the security of their sources and methods, in turn risking UK national security.

**The Guardian**

35. The claimant asserts that there is an inconsistency between his treatment by the UK authorities and the approach taken towards The Guardian which, he believes, shows that there is no urgency here. He relies on the statement by Mr Rusbridger [C5]. The claimant's assertion is incorrect for the following reasons.

36. HMG became aware, through the newspaper's own reporting, that The Guardian was in possession of information passed to it, through a third party, by Mr Snowden. In addition, The Guardian reported that this material included information originating from GCHQ. As members of the Newspaper Publishers Association, which sits on the DPBAC, the Guardian Newspapers are party to this agreement. It was therefore a matter of serious concern to us that initial reporting by the Guardian which appeared in its print edition of 17 June 2013 (and subsequently of 21 June) contained material damaging to the national security of the United Kingdom. HMG was also very concerned that the newspaper also claimed it held much more GCHQ information than the material it had already reported on.

37. HMG was deeply concerned at the prospect of sensitive intelligence material being outside its protection. It was certain that disclosure of this type of information could cause grievous harm to national security and counter-terrorism operations, as well as posing a direct threat to life of UK government employees. The Government decided to engage the newspaper quickly to address our immediate and overriding objective: to mitigate the risk of a potentially catastrophic stream of public reporting of intelligence material.

38. Following publication on 17 June, the actual and potential damage caused was discussed at the highest level of Government leading to direct engagement with the Guardian during the course of that week. These discussions continued to the conclusion of the engagement.

39. Once our principal objective had been achieved, HMG resolved to take all reasonable steps to recover the information and/or remove its potential to cause intended or unintended damage. We wanted to achieve this as quickly as possible. Preferably the material would be retrieved to help us to understand the extent of damage that might be caused by further disclosure and damage that might have occurred already, but that particular concern was, at that stage, of secondary importance behind placing the information beyond the reach of others.

40. HMG was, throughout this unusual situation, trying to observe its duty to protect national security and to avoid any misrepresentation that the Government was seeking to hide embarrassment or stifle legitimate journalism.

41. From a national security perspective we had two specific concerns to manage. There was the direct damage to national security that could flow from the newspaper's reporting, but there was also the wider question of intended or unintended disclosure of the material to third parties, for we were sure that The Guardian would not be able to provide adequate assurance around its security arrangements. HMG was extremely concerned that The Guardian had effectively advertised itself as a target for hostile groups wishing to obtain the underlying data.

42. We were also aware that there could be other parties who might already have access to the information, and that there might be more than one copy of the information, and that these copies could be located outside the UK. So HMG needed to try to avoid its efforts (to secure the material held by The Guardian and prevent damaging disclosures) provoking a more wholesale disclosure by another party.

43. It is important to note that, in seeking to protect the material, HMG was carrying out its duty to protect the public. Over and above the statutory duties of the security and intelligence agencies, one of the first functions of Government is to protect the country and its citizens against threats. It is this overriding public interest which informed the approach HMG took in relation to the aim of making the material safe, above all else. We were also clear that due to these obligations that leaving the material in jeopardy was not an option.

44. Our consideration of the options for making the material safe led us to conclude that, so long as the newspaper showed co-operation, engagement was the best strategy. In reaching this conclusion we were mindful of the following:

    a. Civil action to retrieve the information was an option kept open at all times, but was not considered necessary so long as negotiation with the Guardian was productive, and might risk provoking an irresponsible reaction.

    b. A complaint to the police was considered but, as stated above, HMG was always mindful of its strong wish to avoid any misrepresentation that the Government was seeking to hide embarrassment or stifle legitimate journalism. Had The Guardian failed to co-operate, HMG would have reassessed our initial decision.

45. Having decided upon our strategy, we made a confidential approach to the newspaper. Through a series of discussions we first secured an agreement that the newspaper would not publish a story without first approaching us through the DA Notice Committee or directly. Having achieved this first limited goal our emphasis shifted to working to secure the information.

46. Further discussions led to an agreement with The Guardian Editor, Mr Rusbridger, that the material should be destroyed to make it safe. We made clear to The Guardian from the outset that we were extremely concerned by their possession of our sensitive information and that they should not be holding it. We informed them that we had no confidence in their ability to keep the material safe. Nor could they understand the damage that might flow from its further compromise. We made clear that the information would be targeted by any number of hostile actors and could cause further damage to UK counter terrorism operations.

47. The Guardian appeared to accept our assessment that their continued possession of the information was untenable. The Guardian continued to refuse to hand over the material and would not move on this point. Therefore destruction of the material, under our supervision, was assessed to be the best practicable option, as it immediately prevented further damage as a result of disclosure from their cache and we achieved our objective in this respect. We had acted in good faith, reaching a confidential agreement (now broken by The Guardian) whilst not alerting other parties.

48. Despite agreeing to keep HMG's interaction with The Guardian confidential, the newspaper unilaterally published details on 20 August 2013. The Guardian also revealed on 23 August (in an article titled 'Guardian partners with New York Times over Snowden GCHQ files') that they provided a separate copy of the material to a third party in order to get it outside of the UK's jurisdiction. This is obviously, from a national security perspective, of great concern, for the reasons set out earlier in this witness statement. But it does not mean that the decision by HMG to engage with The Guardian to encourage responsible journalism and the police's decision to stop the claimant are inconsistent.

**Conclusion**

49. This witness statement sets out the urgent need, for both national security reasons and to support the police's criminal investigation, for the police and other agencies to disclose, transfer, examine or otherwise interfere with the material that was seized in order to understand its contents and take steps to mitigate the adverse consequences for the national security of the United Kingdom.

50. The contents of this witness statement are true to the best of my knowledge and belief,

Signed: .....

Dated: 27 August 2013